

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Minoru IKEDA

Serial No. Not yet assigned

Filed: herewith

:  
:  
:  
:  
:  
:

Group Art Unit: Not yet assigned

Examiner: N/A

For: INFORMATION EXCHANGING SYSTEM, INFORMATION COMMUNICATION  
TERMINAL, INFORMATION EXCHANGING METHOD, AND COMPUTER  
PRODUCT



**CLAIM OF PRIORITY AND**  
**TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Assistant Commissioner For Patents  
Washington, D.C. 20231

Dear Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicant hereby claims the  
priority of:

**Japanese Patent Application No. 2001-094347 filed March 28, 2001 and**  
**Japanese Patent Application No. 2001-175874 filed June 11, 2001**

cited in the Declaration of the present application.

The certified copy is submitted herewith.

Respectfully submitted,

LOWE HAUPTMAN GILMAN & BERNER, LLP

Benjamin J. Hauptman  
Registration No. 29,031

1700 Diagonal Road, Suite 310  
Alexandria, Virginia 22314  
(703) 684-1111  
BJH:tmp

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

JC986 U.S. PTO  
09/988237  
11/19/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 3月28日

出 願 番 号

Application Number:

特願2001-094347

出 願 人

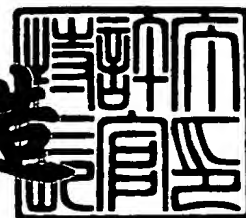
Applicant(s):

池田 実

2001年 8月24日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



出証番号 出証特2001-3076222

【書類名】 特許願

【整理番号】 PIMA-13003

【提出日】 平成13年 3月28日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60

【発明者】

    【住所又は居所】 千葉県船橋市習志野台 2 - 2 1 - 4

    【氏名】 池田 実

【特許出願人】

    【住所又は居所】 千葉県船橋市習志野台 2 - 2 1 - 4

    【氏名又は名称】 池田 実

【代理人】

    【識別番号】 100089118

    【弁理士】

    【氏名又は名称】 酒井 宏明

【選任した代理人】

    【識別番号】 100113103

    【弁理士】

    【氏名又は名称】 香島 拓也

【手数料の表示】

    【予納台帳番号】 036711

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報交換システム、情報通信端末、情報交換方法、および、プログラム

【特許請求の範囲】

【請求項 1】 複数の要素を含む情報を送受信する情報通信端末を用いて上記情報を交換する情報交換システムにおいて、

送信側の情報通信端末は、

上記複数の要素の機密結合度を設定する機密結合度設定手段と、

上記機密結合度設定手段にて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定手段と、

上記分割ルール設定手段にて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割手段と、

上記分割手段にて分割された複数の上記疎結合情報、および、上記分割ルール設定手段にて設定された上記分割ルールを送信する送信手段と、

を備え、

受信側の情報通信端末は、

複数の上記疎結合情報、および、上記分割ルールを受信する受信手段と、

上記受信手段にて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成手段と、

を備えたことを特徴とする情報交換システム。

【請求項 2】 上記送信手段は、

複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティング手段をさらに備え、

上記受信手段は、複数の上記疎結合情報を上記複数の伝送経路から受信することを特徴とする請求項 1 に記載の情報交換システム。

【請求項 3】 上記送信側の情報通信端末は、

上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定手段と、

上記ネーミングルール設定手段にて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化手段と、

上記ネーミングルール設定手段にて設定された上記ネーミングルールを送信するネーミングルール送信手段と、

をさらに備え、

上記受信側の情報通信端末は、

上記ネーミングルールを受信するネーミングルール受信手段と、

上記ネーミングルール受信手段にて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換手段と、

をさらに備えたことを特徴とする請求項 1 に記載の情報交換システム。

【請求項 4】 上記情報は、XML により記載されていることを特徴とする請求項 1 に記載の情報交換システム。

【請求項 5】 上記機密結合度設定手段は、DTD に定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする請求項 4 に記載の情報交換システム。

【請求項 6】 複数の要素を含む情報を送受信する情報通信端末において、上記複数の要素の機密結合度を設定する機密結合度設定手段と、

上記機密結合度設定手段にて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定手段と、

上記分割ルール設定手段にて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割手段と、

上記分割手段にて分割された複数の上記疎結合情報、および、上記分割ルール設定手段にて設定された上記分割ルールを送信する送信手段と、

を備えたことを特徴とする情報通信端末。

【請求項 7】 複数の上記疎結合情報、および、上記分割ルールを受信する受信手段と、

上記受信手段にて受信した上記分割ルールに基づいて、複数の上記疎結合情報

から上記情報を再構成する再構成手段と、

をさらに備えたことを特徴とする請求項 6 に記載の情報通信端末。

【請求項 8】 上記送信手段は、

複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティング手段をさらに備えたことを特徴とする請求項 6 に記載の情報通信端末。

【請求項 9】 上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定手段と、

上記ネーミングルール設定手段にて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化手段と、

上記ネーミングルール設定手段にて設定された上記ネーミングルールを送信するネーミングルール送信手段と、

をさらに備えたことを特徴とする請求項 6 に記載の情報通信端末。

【請求項 10】 上記ネーミングルールを受信するネーミングルール受信手段と、

上記ネーミングルール受信手段にて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換手段と

をさらに備えたことを特徴とする請求項 9 に記載の情報通信端末。

【請求項 11】 上記情報は、XML により記載されていることを特徴とする請求項 6 に記載の情報通信端末。

【請求項 12】 上記機密結合度設定手段は、DTD に定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする請求項 11 に記載の情報通信端末。

【請求項 13】 複数の要素を含む情報を送受信する情報通信端末を用いて上記情報を交換する情報交換システムを用いて実行される情報交換方法において

送信側の情報通信端末において、上記複数の要素の機密結合度を設定する機密結合度設定ステップと、

上記機密結合度設定ステップにおいて設定された上記機密結合度に基づいて、

上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定ステップと、

上記分割ルール設定ステップにおいて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割ステップと、

上記分割ステップにおいて分割された複数の上記疎結合情報、および、上記分割ルール設定ステップにおいて設定された上記分割ルールを受信側の情報通信端末に対して送信する送信ステップと、

上記受信側の情報通信端末において、複数の上記疎結合情報、および、上記分割ルールを受信する受信ステップと、

上記受信ステップにおいて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成ステップと、

を含むことを特徴とする情報交換方法。

【請求項 1 4】 上記送信ステップは、

複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティングステップをさらに含み、

上記受信ステップは、複数の上記疎結合情報を上記複数の伝送経路から受信することを特徴とする請求項 1 3 に記載の情報交換方法。

【請求項 1 5】 上記送信側の情報通信端末において、上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定ステップと、

上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化ステップと、

上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールを上記受信側の情報通信端末に対して送信するネーミングルール送信ステップと

上記受信側の情報通信端末において、上記ネーミングルールを受信するネーミングルール受信ステップと、

上記ネーミングルール受信ステップにおいて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変

換ステップと、

をさらに含むことを特徴とする請求項 1 3 に記載の情報交換方法。

【請求項 1 6】 上記情報は、XML により記載されていることを特徴とする請求項 1 3 に記載の情報交換方法。

【請求項 1 7】 上記機密結合度設定ステップは、DTD に定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする請求項 1 6 に記載の情報交換方法。

【請求項 1 8】 複数の要素を含む情報を送受信する情報通信端末を用いて実行される情報交換方法において、

上記複数の要素の機密結合度を設定する機密結合度設定ステップと、

上記機密結合度設定ステップにおいて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定ステップと、

上記分割ルール設定ステップにおいて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割ステップと、

上記分割ステップにおいて分割された複数の上記疎結合情報、および、上記分割ルール設定ステップにおいて設定された上記分割ルールを送信する送信ステップと、

を含むことを特徴とする情報交換方法。

【請求項 1 9】 複数の上記疎結合情報、および、上記分割ルールを受信する受信ステップと、

上記受信ステップにおいて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成ステップと、

をさらに含むことを特徴とする請求項 1 8 に記載の情報交換方法。

【請求項 2 0】 上記送信ステップは、

複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティングステップをさらに含むことを特徴とする請求項 1 8 に記載の情報交換方法。

【請求項 2 1】 上記要素の名称を別の名称とするためのネーミングルール



を設定するネーミングルール設定ステップと、

上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化ステップと、

上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールを送信するネーミングルール送信ステップと、

をさらに含むことを特徴とする請求項 1 8 に記載の情報交換方法。

【請求項 2 2】 上記ネーミングルールを受信するネーミングルール受信ステップと、

上記ネーミングルール受信ステップにおいて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換ステップと、

をさらに含むことを特徴とする請求項 2 1 に記載の情報交換方法。

【請求項 2 3】 上記情報は、XMLにより記載されていることを特徴とする請求項 1 8 に記載の情報交換方法。

【請求項 2 4】 上記機密結合度設定ステップは、DTDに定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする請求項 2 3 に記載の情報交換方法。

【請求項 2 5】 複数の要素を含む情報を送受信する情報通信端末に情報交換方法を実行させるプログラムにおいて、

上記複数の要素の機密結合度を設定する機密結合度設定ステップと、

上記機密結合度設定ステップにおいて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定ステップと、

上記分割ルール設定ステップにおいて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割ステップと、

上記分割ステップにおいて分割された複数の上記疎結合情報、および、上記分割ルール設定ステップにおいて設定された上記分割ルールを送信する送信ステップと、

を含むことを特徴とするプログラム。

【請求項 2 6】 複数の上記疎結合情報、および、上記分割ルールを受信する受信ステップと、

上記受信ステップにおいて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成ステップと、

をさらに含むことを特徴とする請求項 2 5 に記載のプログラム。

【請求項 2 7】 上記送信ステップは、

複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティングステップをさらに含むことを特徴とする請求項 2 5 に記載のプログラム。

【請求項 2 8】 上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定ステップと、

上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化ステップと、

上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールを送信するネーミングルール送信ステップと、

をさらに含むことを特徴とする請求項 2 5 に記載のプログラム。

【請求項 2 9】 上記ネーミングルールを受信するネーミングルール受信ステップと、

上記ネーミングルール受信ステップにおいて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換ステップと、

をさらに含むことを特徴とする請求項 2 8 に記載のプログラム。

【請求項 3 0】 上記情報は、XML により記載されていることを特徴とする請求項 2 5 に記載のプログラム。

【請求項 3 1】 上記機密結合度設定ステップは、DTD に定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする請求項 3 0 に記載のプログラム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、情報交換システム、情報通信端末、情報交換方法、および、プログラムに関し、特に、XMLにより記載された情報を送受信する情報交換システム、情報通信端末、情報交換方法、および、プログラムに関する。

【0002】

【従来の技術】

インターネットは、利用者にとって極めて安価かつ容易に利用できる通信手段である。しかし、インターネットは、元来オープンなコミュニケーションのために作られ、利用されてきたものであるため、B2B(Business to Business)の企業同士の取引などにおける企業情報や医療情報など秘匿性を要求される分野の情報交換手段には不向きである。そのため、これまでにインターネットの欠点を補い通信の安全性を確保するためのセキュリティ手段がいくつか開発されている。

【0003】

【発明が解決しようとする課題】

しかしながら、従来のインターネットにおけるセキュリティ手段は、導入が高価であり、複雑で手軽に利用できるものではなかったという問題点を有していた。

【0004】

また、インターネットで広く用いられる比較的導入が容易なSSL(Secure Sockets Layer)等の簡易な暗号システムを用いる場合には、第3者により比較的容易に暗号鍵を見破られる恐れがあるという問題点を有していた。

【0005】

また、B2B等の情報交換においては、WWWコンソーシアム(W3C)が標準化を進めているXML(Extensible Markup Language)をデータの記述言語として用いる場合が多くなっている。XMLにより作成される情報は、要素(element)を基本単位とする。「要素」は、要素に関連付けられた名前であって開始タグと終了タグの両方に記述される「要素名

(element name)」、要素に関連付けられた内容であって開始タグと終了タグの間に記述される「要素内容 (element content)」、および、任意に指定される「属性 (attribute)」からなる。ここで、要素は、DTD (Document Type Definition) において定義される。すなわち、XMLは、情報 (文書) の構造等をDTDという文書型定義ファイルにして交換することができる。これにより、利用者は、情報交換される文書の表現方法の指定や文章中の文字列に意味を付加するような独自のタグを作成して用いることができる。このようにXMLは高度な構造表現と明快な内容表現力を備えている。

## 【0006】

しかしながら、このように優れた性質をもつXMLであるが、逆に漏洩した場合は、その情報内容の解析が他の表現手段よりも容易となる。すなわち、XMLを用いた情報交換は、第三者がDTDとXML文書により情報 (文書) の内容を容易に推測することができるので、HTMLを用いた情報交換に比べて、第三者により情報交換される情報 (文書) の内容を知られる可能性は高くなるという問題点がある。

## 【0007】

このように、従来のシステム等は数々の問題点を有しており、その結果、利用者のいずれにとっても、利便性が悪く、また、セキュリティが悪いものであった。

本発明は上記問題点に鑑みてなされたもので、比較的手軽な暗号化のような機密保護に加えて、万一それが破られても情報の秘匿性の保持を可能とするものであり、オープンなインターネットを利用しつつ秘匿性が高い情報の交換を安価に実現することのできる、情報交換システム、情報通信端末、情報交換方法、および、プログラムを提供することを目的としている。

## 【0008】

## 【課題を解決するための手段】

このような目的を達成するため、請求項1に記載の情報交換システムは、複数の要素を含む情報を送受信する情報通信端末を用いて上記情報を交換する情報交

換システムにおいて、送信側の情報通信端末は、上記複数の要素の機密結合度を設定する機密結合度設定手段と、上記機密結合度設定手段にて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定手段と、上記分割ルール設定手段にて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割手段と、上記分割手段にて分割された複数の上記疎結合情報、および、上記分割ルール設定手段にて設定された上記分割ルールを送信する送信手段とを備え、受信側の情報通信端末は、複数の上記疎結合情報、および、上記分割ルールを受信する受信手段と、上記受信手段にて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成手段とを備えたことを特徴とする。

## 【 0 0 0 9 】

このシステムによれば、送信側の情報通信端末は、複数の要素の機密結合度を設定し、設定された機密結合度に基づいて、情報を複数の疎結合情報に分割するための分割ルールを設定し、設定された分割ルールに基づいて、情報を複数の上記疎結合情報に分割し、分割された複数の疎結合情報、および、設定された分割ルールを送信し、受信側の情報通信端末は、複数の疎結合情報、および、分割ルールを受信し、受信した分割ルールに基づいて、複数の疎結合情報から情報を再構成するので、送受信される情報の秘匿性を高めることができる。

## 【 0 0 1 0 】

また、本発明は情報交換システムに関するものであり、請求項 2 に記載の情報交換システムは、請求項 1 に記載の情報交換システムにおいて、上記送信手段は、複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティング手段をさらに備え、上記受信手段は、複数の上記疎結合情報を上記複数の伝送経路から受信することを特徴とする。

## 【 0 0 1 1 】

これは送信手段の一例を一層具体的に示すものである。このシステムによれば、複数の疎結合情報を複数の伝送経路を用いて送信し、複数の疎結合情報を複数の伝送経路から受信するので、機密結合度が下げられて生成された複数の疎結合情報をそれぞれ別の通信路を用いて情報交換することができる。また、疎結合情

報の対応関係を隠蔽し、送受信される情報の秘匿性をさらに高めることができる。

#### 【 0 0 1 2 】

また、本発明は情報交換システムに関するものであり、請求項 3 に記載の情報交換システムは、請求項 1 に記載の情報交換システムにおいて、上記送信側の情報通信端末は、上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定手段と、上記ネーミングルール設定手段にて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化手段と、上記ネーミングルール設定手段にて設定された上記ネーミングルールを送信するネーミングルール送信手段とをさらに備え、上記受信側の情報通信端末は、上記ネーミングルールを受信するネーミングルール受信手段と、上記ネーミングルール受信手段にて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換手段とをさらに備えたことを特徴とする。

#### 【 0 0 1 3 】

このシステムによれば、送信側の情報通信端末は、要素の名称を別の名称とするためのネーミングルールを設定し、設定されたネーミングルールに基づいて、情報の要素の名称を別の名称にするとともに、設定されたネーミングルールを送信する。受信側の情報通信端末は、ネーミングルールを受信するとともに、受信したネーミングルールに基づいて、別名化された情報の要素の名称を元の名称に変換するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

#### 【 0 0 1 4 】

また、請求項 4 における情報交換システムは、請求項 1 に記載の情報交換システムにおいて、情報が XML により記載されたものであることを特徴にする。

#### 【 0 0 1 5 】

これは情報の一例を一層具体的に示すものである。このシステムによれば、情報が XML により記載されたものであるので、XML データの分解・再構成の容

易性を活かしてXMLデータの機密結合度を下げ、秘匿性を高めることができる。

## 【 0 0 1 6 】

請求項5に記載の情報交換システムは、請求項4に記載の情報交換システムにおいて、上記機密結合度設定手段は、DTDに定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする。

## 【 0 0 1 7 】

これは機密結合度設定手段の一例を一層具体的に示すものである。このシステムによれば、DTDに定義されている要素について、要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定するので、DTDに定義されたXML情報の要素の内容に基づいて、効率的に機密結合度を設定できる。

## 【 0 0 1 8 】

また、本発明は情報通信端末に関するものであり、請求項6に記載の情報通信端末は、複数の要素を含む情報を送受信する情報通信端末において、上記複数の要素の機密結合度を設定する機密結合度設定手段と、上記機密結合度設定手段にて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定手段と、上記分割ルール設定手段にて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割手段と、上記分割手段にて分割された複数の上記疎結合情報、および、上記分割ルール設定手段にて設定された上記分割ルールを送信する送信手段とを備えたことを特徴とする。

## 【 0 0 1 9 】

この端末によれば、複数の要素の機密結合度を設定し、設定された機密結合度に基づいて、情報を複数の疎結合情報に分割するための分割ルールを設定し、設定された分割ルールに基づいて、情報を複数の疎結合情報に分割し、分割された複数の疎結合情報、および、設定された分割ルールを送信するので、送受信される情報の秘匿性を高めることができる。

## 【 0 0 2 0 】

また、請求項 7 に記載の情報通信端末は、請求項 6 に記載の情報通信端末において、複数の上記疎結合情報、および、上記分割ルールを受信する受信手段と、上記受信手段にて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成手段とをさらに備えたことを特徴とする。

【 0 0 2 1 】

この端末によれば、複数の疎結合情報、および、分割ルールを受信し、受信した分割ルールに基づいて、複数の疎結合情報から情報を再構成するので、送受信される情報の秘匿性を高めることができる。

【 0 0 2 2 】

また、請求項 8 に記載の情報通信端末は、請求項 6 に記載の情報通信端末において、上記送信手段は、複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティング手段をさらに備えたことを特徴とする。

【 0 0 2 3 】

これは送信手段の一例を一層具体的に示すものである。この端末によれば、送信手段は、複数の疎結合情報を複数の伝送経路を用いて送信するので、機密結合度が下げられて生成された複数の疎結合情報をそれぞれ別の通信路を用いて情報交換することができる。また、疎結合情報の対応関係を隠蔽し、送受信される情報の秘匿性をさらに高めることができる。

【 0 0 2 4 】

また、請求項 9 に記載の情報通信端末は、請求項 6 に記載の情報通信端末において、上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定手段と、上記ネーミングルール設定手段にて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化手段と、上記ネーミングルール設定手段にて設定された上記ネーミングルールを送信するネーミングルール送信手段とをさらに備えたことを特徴とする。

【 0 0 2 5 】

この端末によれば、要素の名称を別の名称とするためのネーミングルールを設定し、設定されたネーミングルールに基づいて、情報の要素の名称を別の名称にし、設定されたネーミングルールを送信するので、オリジナルの情報から別の名



称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

【 0 0 2 6 】

また、請求項 1 0 に記載の情報通信端末は、請求項 9 に記載の情報通信端末において、上記ネーミングルールを受信するネーミングルール受信手段と、上記ネーミングルール受信手段にて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換手段とをさらに備えたことを特徴とする。

【 0 0 2 7 】

この端末によれば、ネーミングルールを受信し、受信した上記ネーミングルールに基づいて、別名化された情報の要素の名称を元の名称に変換するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

【 0 0 2 8 】

また、請求項 1 1 に記載の情報通信端末は、請求項 6 に記載の情報通信端末において、上記情報は、XMLにより記載されていることを特徴とする。

【 0 0 2 9 】

これは情報の一例を一層具体的に示すものである。このシステムによれば、情報は、XMLにより記載されているので、XMLデータの分解・再構成の容易性を活かしてXMLデータの機密結合度を下げ、秘匿性を高めることができる。

【 0 0 3 0 】

また、請求項 1 2 に記載の情報通信端末は、請求項 1 1 に記載の情報通信端末において、上記機密結合度設定手段は、DTDに定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする。

【 0 0 3 1 】

これは機密結合度設定手段の一例を一層具体的に示すものである。このシステ

ムによれば、DTDに定義されている要素について、要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定するので、DTDに定義されたXML情報の要素の内容に基づいて、効率的に機密結合度を設定できる。

#### 【0032】

また、本発明は情報交換方法に関するものであり、請求項13に記載の情報交換方法は、複数の要素を含む情報を送受信する情報通信端末を用いて上記情報を交換する情報交換システムを用いて実行される情報交換方法において、送信側の情報通信端末において、上記複数の要素の機密結合度を設定する機密結合度設定ステップと、上記機密結合度設定ステップにおいて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定ステップと、上記分割ルール設定ステップにおいて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割ステップと、上記分割ステップにおいて分割された複数の上記疎結合情報、および、上記分割ルール設定ステップにおいて設定された上記分割ルールを受信側の情報通信端末に対して送信する送信ステップと、上記受信側の情報通信端末において、複数の上記疎結合情報、および、上記分割ルールを受信する受信ステップと、

上記受信ステップにおいて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成ステップとを含むことを特徴とする。

#### 【0033】

この方法によれば、送信側の情報通信端末において、複数の要素の機密結合度を設定し、設定された機密結合度に基づいて、情報を複数の疎結合情報に分割するための分割ルールを設定し、設定された分割ルールに基づいて、情報を複数の疎結合情報に分割し、分割された複数の疎結合情報、および、設定された分割ルールを受信側の情報通信端末に対して送信し、受信側の情報通信端末において、複数の疎結合情報、および、分割ルールを受信し、受信した分割ルールに基づいて、複数の疎結合情報から情報を再構成するので、送受信される情報の秘匿性を高めることができる。

#### 【0034】

また、請求項14に記載の情報交換方法は、請求項13に記載の情報交換方法

において、上記送信ステップは、複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティングステップをさらに含み、上記受信ステップは、複数の上記疎結合情報を上記複数の伝送経路から受信することを特徴とする。

## 【 0 0 3 5 】

これは送信ステップの一例を一層具体的に示すもので、この方法によれば、複数の疎結合情報を複数の伝送経路を用いて送信し、複数の疎結合情報を複数の伝送経路から受信するので、機密結合度が下げられて生成された複数の疎結合情報をそれぞれ別の通信路を用いて情報交換することができる。また、疎結合情報の対応関係を隠蔽し、送受信される情報の秘匿性をさらに高めることができる。

## 【 0 0 3 6 】

また、請求項 1 5 に記載の情報交換方法は、請求項 1 3 に記載の情報交換方法において、上記送信側の情報通信端末において、上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定ステップと、上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化ステップと、上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールを上記受信側の情報通信端末に対して送信するネーミングルール送信ステップと、上記受信側の情報通信端末において、上記ネーミングルールを受信するネーミングルール受信ステップと、上記ネーミングルール受信ステップにおいて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換ステップとをさらに含むことを特徴とする。

## 【 0 0 3 7 】

この方法によれば、送信側の情報通信端末において、要素の名称を別の名称とするためのネーミングルールを設定し、設定された上記ネーミングルールに基づいて、情報の要素の名称を別の名称にし、設定されたネーミングルールを受信側の情報通信端末に対して送信し、受信側の情報通信端末において、ネーミングルールを受信し、受信したネーミングルールに基づいて、別名化された情報の要素の名称を元の名称に変換するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすること

ができ、送受信される情報の秘匿性をさらに高めることができる。

【 0 0 3 8 】

また、請求項 1 6 における情報交換方法は、請求項 1 3 に記載の情報交換方法において、情報が XML により記載されたものであることを特徴とする。

【 0 0 3 9 】

これは情報の一例を一層具体的に示すものである。この方法によれば、情報が XML により記載されたものであるので、XML データの分解・再構成の容易性を活かして XML データの機密結合度を下げ、秘匿性を高めることができる。

【 0 0 4 0 】

また、請求項 1 7 に記載の情報交換方法は、請求項 1 6 に記載の情報交換方法において、上記機密結合度設定ステップは、DTD に定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする。

【 0 0 4 1 】

これは機密結合度設定ステップの一例を一層具体的に示すものである。この方法によれば、DTD に定義されている要素について、要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定するので、DTD に定義された XML 情報の要素の内容に基づいて、効率的に機密結合度を設定できる。

【 0 0 4 2 】

また、本発明は情報交換方法に関するものであり、請求項 1 8 に記載の情報交換方法は、複数の要素を含む情報を送受信する情報通信端末を用いて実行される情報交換方法において、上記複数の要素の機密結合度を設定する機密結合度設定ステップと、上記機密結合度設定ステップにおいて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定ステップと、上記分割ルール設定ステップにおいて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割ステップと、上記分割ステップにおいて分割された複数の上記疎結合情報、および、上記分割ルール設定ステップにおいて設定された上記分割ルールを送信する送信ステップとを含むことを特徴とする。

## 【 0 0 4 3 】

この方法によれば、複数の要素の機密結合度を設定し、設定された上記機密結合度に基づいて、情報を複数の疎結合情報に分割するための分割ルールを設定し、設定された分割ルールに基づいて、情報を複数の上記疎結合情報に分割し、分割された複数の疎結合情報、および、設定された分割ルールを送信するので、送受信される情報の秘匿性を高めることができる。

## 【 0 0 4 4 】

また、請求項 1 9 に記載の情報交換方法は、請求項 1 8 に記載の情報交換方法において、複数の上記疎結合情報、および、上記分割ルールを受信する受信ステップと、上記受信ステップにおいて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成ステップとをさらに含むことを特徴とする。

## 【 0 0 4 5 】

この方法によれば、複数の疎結合情報、および、分割ルールを受信し、受信した分割ルールに基づいて、複数の疎結合情報から情報を再構成するので、送受信される情報の秘匿性をさらに高めることができる。

## 【 0 0 4 6 】

また、請求項 2 0 に記載の情報交換方法は、請求項 1 8 に記載の情報交換方法において、上記送信ステップは、複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティングステップをさらに含むことを特徴とする。

## 【 0 0 4 7 】

これは送信ステップの一例を一層具体的に示すものである。この方法によれば、複数の疎結合情報を複数の伝送経路を用いて送信するので、機密結合度が下げられて生成された複数の疎結合情報をそれぞれ別の通信路を用いて情報交換することができる。また、疎結合情報の対応関係を隠蔽し、送受信される情報の秘匿性をさらに高めることができる。

## 【 0 0 4 8 】

また、請求項 2 1 に記載の情報交換方法は、請求項 1 8 に記載の情報交換方法において、上記要素の名称を別の名称とするためのネーミングルールを設定する

ネーミングルール設定ステップと、上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化ステップと、上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールを送信するネーミングルール送信ステップとをさらに含むことを特徴とする。

【 0 0 4 9 】

この方法によれば、要素の名称を別の名称とするためのネーミングルールを設定し、設定されたネーミングルールに基づいて、情報の要素の名称を別の名称にし、設定されたネーミングルールを送信するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

【 0 0 5 0 】

また、請求項 2 2 に記載の情報交換方法は、請求項 2 1 に記載の情報交換方法において、上記ネーミングルールを受信するネーミングルール受信ステップと、上記ネーミングルール受信ステップにおいて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換ステップとをさらに含むことを特徴とする。

【 0 0 5 1 】

この方法によれば、ネーミングルールを受信し、受信したネーミングルールに基づいて、別名化された情報の要素の名称を元の名称に変換するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

【 0 0 5 2 】

また、請求項 2 3 に記載の情報交換方法は、請求項 1 8 に記載の情報交換方法において、上記情報は、XMLにより記載されていることを特徴とする。

【 0 0 5 3 】

これは情報の一例を一層具体的に示すものである。この方法によれば、情報は

、XMLにより記載されているので、XMLデータの分解・再構成の容易性を活かしてXMLデータの機密結合度を下げ、秘匿性を高めることができる。

## 【 0 0 5 4 】

また、請求項 2 4 に記載の情報交換方法は、請求項 2 3 に記載の情報交換方法において、上記機密結合度設定ステップは、DTDに定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする。

## 【 0 0 5 5 】

これは機密結合度設定ステップの一例を一層具体的に示すものである。この方法によれば、DTDに定義されている要素について、要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定するので、DTDに定義されたXML情報の要素の内容に基づいて、効率的に機密結合度を設定できる。

## 【 0 0 5 6 】

また、本発明は、情報通信端末に情報交換方法を実行させるプログラムに関するものであり、請求項 2 5 に記載のプログラムは、複数の要素を含む情報を送受信する情報通信端末に情報交換方法を実行させるプログラムにおいて、上記複数の要素の機密結合度を設定する機密結合度設定ステップと、上記機密結合度設定ステップにおいて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定ステップと、上記分割ルール設定ステップにおいて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割ステップと、上記分割ステップにおいて分割された複数の上記疎結合情報、および、上記分割ルール設定ステップにおいて設定された上記分割ルールを送信する送信ステップとを含むことを特徴とする。

## 【 0 0 5 7 】

このプログラムによれば、複数の要素の機密結合度を設定し、設定された機密結合度に基づいて、情報を複数の疎結合情報に分割するための分割ルールを設定し、設定された分割ルールに基づいて、情報を複数の上記疎結合情報に分割し、分割された複数の疎結合情報、および、設定された分割ルールを送信するので、

送受信される情報の秘匿性を高めることができる。

【 0 0 5 8 】

また、請求項 2 6 に記載のプログラムは、請求項 2 5 に記載のプログラムにおいて、複数の上記疎結合情報、および、上記分割ルールを受信する受信ステップと、上記受信ステップにおいて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成ステップとをさらに含むことを特徴とする。

【 0 0 5 9 】

このプログラムによれば、複数の疎結合情報、および、分割ルールを受信し、受信した分割ルールに基づいて、複数の疎結合情報から情報を再構成するので、送受信される情報の秘匿性を高めることができる。

【 0 0 6 0 】

また、請求項 2 7 に記載のプログラムは、請求項 2 5 に記載のプログラムにおいて、上記送信ステップは、複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティングステップをさらに含むことを特徴とする。

【 0 0 6 1 】

これは送信ステップの一例を一層具体的に示すものである。このプログラムによれば、複数の疎結合情報を複数の伝送経路を用いて送信するので、機密結合度が下げられて生成された複数の疎結合情報をそれぞれ別の通信路を用いて情報交換することができる。また、疎結合情報の対応関係を隠蔽し、送受信される情報の秘匿性をさらに高めることができる。

【 0 0 6 2 】

また、請求項 2 8 に記載のプログラムは、請求項 2 5 に記載のプログラムにおいて、上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定ステップと、上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化ステップと、上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールを送信するネーミングルール送信ステップとをさらに含むことを特徴とする。



【0063】

このプログラムによれば、要素の名称を別の名称とするためのネーミングルールを設定し、設定されたネーミングルールに基づいて、情報の要素の名称を別の名称にし、設定されたネーミングルールを送信するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

【0064】

また、請求項29に記載のプログラムは、請求項28に記載のプログラムにおいて、上記ネーミングルールを受信するネーミングルール受信ステップと、上記ネーミングルール受信ステップにおいて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換ステップとをさらに含むことを特徴とする。

【0065】

このプログラムによれば、ネーミングルールを受信し、受信したネーミングルールに基づいて、別名化された情報の上記要素の名称を元の名称に変換するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

【0066】

また、請求項30に記載のプログラムは、請求項25に記載のプログラムにおいて、上記情報は、XMLにより記載されていることを特徴とする。

【0067】

これは情報の一例を一層具体的に示すものである。このプログラムによれば、情報は、XMLにより記載されているので、XMLデータの分解・再構成の容易性を活かしてXMLデータの機密結合度を下げ、秘匿性を高めることができる。

【0068】

また、請求項31に記載のプログラムは、請求項30に記載のプログラムにおいて、上記機密結合度設定ステップは、DTDに定義されている上記要素につい

て、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする。

#### 【 0 0 6 9 】

これは機密結合度設定ステップの一例を一層具体的に示すものである。このプログラムによれば、DTDに定義されている要素について、要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定するので、DTDに定義されたXML情報の要素の内容に基づいて、効率的に機密結合度を設定できる。

#### 【 0 0 7 0 】

##### 【発明の実施の形態】

以下に、本発明にかかる情報交換システム、情報通信端末、情報交換方法、および、プログラムの実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。

特に、以下の実施の形態においては、本発明を、XMLに適用した例について説明するが、この場合に限られず、SGMLやHTML等のごとく、所定の情報に対してタグ等により属性等を定義することができる全ての記述言語において、同様に適用することできる。

#### 【 0 0 7 1 】

##### （本システムの概要）

以下、本システムの概要について説明し、その後、本システムの構成および処理等について詳細に説明する。図1は本システムの全体構成の一例を示すブロック図であり、また、図2は本システムの概要を示す概念図であり、それぞれ該システム構成のうち本発明に関係する部分のみを概念的に示している。

#### 【 0 0 7 2 】

本システムは、図1に示すように、概略的に、各情報通信端末100がネットワーク300を介して通信可能に接続して構成されている。ここで、情報通信端末100は、既知のパーソナルコンピュータ、ワークステーション、家庭用ゲーム装置、インターネットTV、PHS端末、携帯端末、移動体通信端末、PDA等の情報処理端末等の情報処理装置にプリンタやモニタやイメージスキャナ等の

周辺装置を必要に応じて接続し、該情報処理装置にウェブ情報のブラウジング機能や電子メール機能や後述する各機能を実現させるソフトウェア（プログラム、データ等を含む）を実装することにより実現してもよい。

【0073】

このシステムは、概略的に、以下の基本的特徴を有する。すなわち、情報通信端末100から他の情報通信端末100に対して、情報がネットワーク300を介して提供される。

このうち、情報は、一例としてXMLにより記述されたものであり、DTD（文書型定義）にて定義されたタグ等のメタデータを含む。これらの情報は、情報通信端末100、または、他の装置により生成され、情報通信端末100に蓄積される。

【0074】

本システムは、図2に示すように、送信側の情報通信端末100が設定する分解ルールおよび再構成ルールにより、情報が送信側の情報通信端末100において分解され、受信側の情報通信端末100において再構成される。これにより、既存のシステムやアプリケーションに対して影響を与えず、かつ簡易に導入することができ、高い安全性を得ることができるようになる。

以下に、本システムの情報通信端末100における分解ルールおよび再構成ルールの設定について、その概念を説明する。

【0075】

（1）機密結合度

まず始めに、「機密結合度」の概念を導入する。

上述したように、XMLにより作成される情報は、DTDにおいて定義された要素（element）を基本単位とする。上述したように、DTDにおいて、各要素の名称、内容、属性等が定義される。

【0076】

ここで、交換情報を構成する要素（element）の組合せにより、利用者が期待する機密レベルが異なることが多い。たとえば、企業情報のうち、企業名や社長名は、公開されている情報であるため、その要素を組み合わせた情報は、

機密レベルが低い（単なる公開されている情報の結合に過ぎないため）。また、欠損額等の非公開の要素について、その情報のみを交換する場合には、漏洩されても何処の企業の欠損額であるかは特定できないため実害は少ない。

【0077】

しかしながら、非公開の要素と公開された要素とを結合させた場合には、その内容が漏洩されると公開情報に基づいて非公開の要素が詳細に特定されてしまう恐れが強い。

【0078】

そこで、本システムでは、特定の要素の組合せ毎に「機密結合度」を定義することにより、要素の結合を機密レベルの観点からチェックする。

【0079】

すなわち、本システムは、DTDにおいて定義された各要素について、その要素の名称、内容、属性等に基づいて他の要素と組み合わせた場合の機密結合度を指定する。「機密結合度」は、複数の要素を結合させた場合に、その要素の組合せにより情報の機密性が高くなるか否かを示す値であり、例えば、機密性が高まるにつれて高い数値を設定する。例えば、各要素の名称、内容、属性等をモニタに表示して、利用者に表示された要素の組み合わせ毎に機密結合度を指定させてもよく、また、情報通信端末100が各要素の名称、内容、属性等の情報に基づいて自動的に機密結合度を指定してもよい。

【0080】

ここで、情報通信端末100が各要素の名称、内容、属性等の情報に基づいて自動的に機密結合度を指定する場合の一例を説明する。各要素に必須の属性として、要素内容が公開情報か否かに関する情報（以下「公開属性」という）をDTDにおいて定義する。そして、情報通信端末100は、各要素の公開属性を判断して、公開情報となる要素と非公開情報となる要素との機密結合度を、自動的に高く設定する。

【0081】

なお、機密結合度は、2つの要素の関係に限定されるものではなく、例えば、3つ以上の要素が組み合わさって初めて機密性が高くなる場合には、3つ以上の

要素の組み合わせで機密度を高く設定する。

【0082】

図6は、本システムにおける機密結合度の定義の一例を示す概念図である。

本図において、オリジナルのXMLの情報601は、要素として企業名と社長名と当季欠損額とを含んでいる。ここで、利用者等は、企業名と社長の名前は公示されているものであり機密結合度が低いと定義する。一方、企業の欠損額は秘匿性が高いので企業名と企業の欠損額の組合せは機密結合度が高いと定義する。

【0083】

仮に、この3つの要素を、機密結合度の高・低に従って分割する分割ルールを生成し、この分割ルールに基づいて、企業名および社長名の組合せを含む情報602と、欠損額の情報603とに2分割すると、この両者の機密結合度は低下する。つまり、2つに分割された情報は、両者の対応関係が明らかにならない限り機密的な結合が疎であり、全体として機密結合度が低くなる。

【0084】

本システムは、XMLデータの分解・再構成の容易性を活かしてXMLデータの機密結合度を下げ、秘匿性を高めるものである。ここで、結合度を下げる目的で分割したXMLデータを「疎結合XMLデータ」と称する。また、結合ルール604（すなわち、疎結合XMLと密結合XMLとの変換ルールであり、後述する分解ルールおよび再構成ルールとなるものである）を、リポジトリやDTDファイルや他のファイルに記録して相互に交換することにより、当事者同士は情報を再構成し確認することができる。

【0085】

（2）疎結合XMLデータのマルチルーティング

上述したように、機密結合度が下げられて生成された複数の疎結合XMLデータは、それぞれを別の通信路を用いて情報の交換を行うことにより、両者の対応関係を隠蔽し、機密の保護をより完全にすることができる。このように、本システムでは、生成した疎結合XMLデータを、別の通信路を用いてマルチルーティングすることにより、セキュリティを高めている。ここで、ルーティング数は可変とする。

## 【 0 0 8 6 】

図 7 は、本発明の疎結合 XML データのマルチルーティングの概要を示す概念図である。

本図に示すように、オリジナルの XML データは、DTD と、利用者等に指定された機密結合度とから生成されたルールに従って（ステップ S 7 0 1）、複数の疎結合 XML に分解され（ステップ S 7 0 3）、複数の伝送経路を経て送信側に送られる（ステップ S 7 0 4）。

受信側は、複数の伝送経路から受け取った疎結合 XML データを、別途送られてきているルールに基づいて（ステップ S 7 0 2）、再構成し、オリジナル XML と同一の XML データを得る（ステップ S 7 0 5）。

## 【 0 0 8 7 】

## （ 3 ） 要素名の別名化

XML は、上述したように高度な構造表現と明快な内容表現力を備えている。そのように優れた性質をもつ XML ではあるが、逆に漏洩した場合は、その情報内容の解析が他の表現手段よりずっと容易となる。特に、要素名は、運用上その要素の内容を直接的に示す場合が多いため、その要素名から要素内容を容易に推測することができる。

## 【 0 0 8 8 】

従って、本システムでは、要素名の別名化を行う。この別名化の機能は、オリジナルの XML から別の名称と構造を持つ XML を生成するものである。この機能によりオリジナル情報の推定を困難にする。

## 【 0 0 8 9 】

図 8 は、本発明の要素名の別名化の概要を示す概念図である。

上述したように、密結合 XML データから、疎結合 XML データ（8 0 1 および 8 0 2）と、結合ルール 8 0 3 とが生成されると、要素名について別名化を行う。「別名化」とは、ネーミングルールに基づいて、要素名を対応する別名に置換することという。

## 【 0 0 9 0 】

例えば、本図に示すように、「企業名」を「AAA」に、「社長名」を「BB

B」に、また、「当季欠損額」を「XYZ」に置換する対応表に基づいたネーミングルールを設定し、別名化したXML（以下「別名XML」と称する）804および805を作成し、結合ルールとネーミングルールとを一組の情報806にして管理する。

#### 【0091】

ここで、ネーミングルールは、上述した対応表を用いた変換によるものでもよく、また、ハッシュ関数等の数学的アルゴリズムを用いた変換によるものでもよい。

#### 【0092】

（システム構成）

以下、このような基本的特徴を具現化するための、本システムの構成について説明する。

#### 【0093】

（システム構成—情報通信端末100）

まず、情報通信端末100の構成について説明する。図3は、本発明が適用される情報通信端末100の構成の一例を示すブロック図であり、該構成のうち本発明に関係する部分のみを概念的に示している。図3において情報通信端末100は、概略的に、情報通信端末100の全体を統括的に制御するCPU等の制御部102、通信回線等に接続されるルータ等の通信装置（図示せず）に接続される通信制御インタフェース部104、入出力装置（図示せず）に接続される入出力制御インタフェース部108、および、各種のデータを格納する記憶部106を備えて構成されており、これら各部は任意の通信路を介して通信可能に接続されている。さらに、この情報通信端末100は、ルータ等の通信装置および専用線等の有線または無線の通信回線を介して、ネットワーク300に通信可能に接続されている。

#### 【0094】

記憶部106は、固定ディスク装置等のストレージ手段であり、各種処理やウェブサイト提供に用いる各種のプログラムやテーブルやファイルやデータベースやウェブページ用ファイル等を格納する。情報通信端末100の記憶部106に

は、例えば、DTDやXMLデータやスキーマのリポジトリ、結合ルールやネーミングルール等の各種のルール情報等が格納される。

【0095】

また、図3において、通信制御インタフェース部104は、情報通信端末100とネットワーク300（またはルータ等の通信装置）との間における通信制御を行う。すなわち、通信制御インタフェース部104は、他の端末と通信回線を介してデータを通信する機能を有する。

【0096】

また、図3において、入出力制御インタフェース部108は、入力装置や出力装置の制御を行う。ここで、出力装置としては、モニタ（家庭用テレビを含む）の他、スピーカを用いることができる（なお、以下においては出力装置をモニタとして記載する）。また、入力装置としては、キーボード、マウス、および、マイク等を用いることができる。また、モニタも、マウスと協働してポインティングデバイス機能を実現する。

【0097】

また、図3において、制御部102は、OS（Operating System）等の制御プログラム、各種の処理手順等を規定したプログラム、および所要データを格納するための内部メモリを有し、これらのプログラム等により、種々の処理を実行するための情報処理を行う。制御部102は、機能概念的に、設定モジュール102a、実行モジュール102b、および、XMLミドルウェア102cを備えて構成されている。なお、これら各部によって行なわれる処理の詳細については、後述する。

【0098】

（システム構成—情報通信端末100のソフトウェア構成）

次に、このように構成された情報通信端末100のソフトウェア構成について、図4を参照して説明する。図4は、本発明が適用される情報通信端末100の102において実行されるソフトウェア構成の一例を示すブロック図であり、該構成のうち本発明に関係する部分のみを概念的に示している。図4において情報通信端末100は、概略的に、設定モジュール102aと、実行モジュール10



2bと、XMLミドルウェア102cとを含んで構成される。

【0099】

図4において、設定モジュール102aは、上述した結合ルールやネーミングルール等のルールを設定する機能を有し、以下に説明する、DTDリポジトリと、ルールビルダと、ルール設定処理部とを含んで構成される。

【0100】

(1) DTDリポジトリ

DTDリポジトリは、XMLデータのメタデータの記憶手段である。ここで、複数のXMLビジネスデータを扱う利用環境を想定すると、DTDをまとめて体系的に管理・利用を行う仕組みが必要となる。DTDリポジトリは、大量のDTDをネットワーク上で共同利用するための道具であり、DTDやスキーマ等を管理する。DTDリポジトリは、一般に、情報入出力インタフェース機能、記憶領域の管理機能を備えるソフトウェアにより構成される。

【0101】

(2) ルールビルダ

上述したように、データの利用者は、データ内容や機密のレベルを定め、それを機密結合度として指定する。ルールビルダは、利用者の指定内容とDTDとを参照しながら結合ルールやネーミングルール等の各種のルールを自動的に生成する。

【0102】

(3) ルール設定処理部

ルール設定処理部は、モニタにルールの設定画面（例えば、各要素の名称、内容、属性等の表示領域と、各要素の機密結合度の入力領域とを含む画面）を表示して、利用者が各種のルールを入力装置を介して設定するための処理を行う。

【0103】

また、図4において実行モジュール102bは、XMLミドルウェア102cから受信した情報を、設定モジュール102aにより設定された各種のルールに従って、処理を実行する機能を有し、以下に説明する、パーサと、デバイダと、IPアロケータと、IP/ポートマネジャーと、サーバと、コンストラクタと、

入出力コネクタとを含んで構成される。

【0104】

(1) パーサ

パーサは、W3CのXML規格に準拠した構文解析を行い、トークンを作成して、デバイダに引き渡す機能を有する。すなわち、パーサは、テキストを解釈し、その論理的意味を判断し、その意味を表すプログラミングデータ構造を作成するソフトウェアプログラムである。なお、本システムは、ツリーベースのパーサであっても、イベントベースのパーサであってもよい。

また、受信時には、別名化された要素名をネーミングルールに基づいて元の要素名に変換する機能を有する。

【0105】

(2) デバイダ

デバイダは、設定モジュールが生成したルールに従って、XMLデータの分割を行う機能を有する。また、送信時には、要素名の別名化を行う機能を有する。

【0106】

(3) IPアロケータ

IPアロケータは、分割数に応じたIPの割当や、開放を行う機能を有する。

【0107】

(4) IP／ポートマネジャー

IP／ポートマネジャーは、IPやポートを複数利用する際には資源を動的に割り当てることが必要となるため、これらの資源の監視と管理を行う機能を有する。

【0108】

(5) サーバ

サーバは、Web、Ftp、smtpなどのサービスするプロトコルに対応するサーバ機能を有する。

【0109】

(6) コンストラクタ

コンストラクタは、パーサが生成したトークンを受け取り、再構成ルールに従

ってXMLデータを再構成する機能を有する。

【0110】

(7) 入出力コネクタ

入出力コネクタは、実行モジュールの外側にあるアプリケーションシステムとのコミュニケーションを行う機能を有する。

【0111】

図4において、XMLミドルウェア102cは、XMLデータを処理するミドルウェアであり、利用者が実行するアプリケーションプログラムから、交換情報となるXMLデータを実行モジュール102bに渡す機能を有する。また、実行モジュール102bにおいて他の情報通信端末100から受信したXMLデータをアプリケーションプログラムに渡す機能を有する。

【0112】

(情報通信端末100における情報の流れ)

このように構成された情報通信端末100における情報の流れを図5、図9および図10を用いて説明する。

【0113】

図5は、情報通信端末100における情報の流れの概要を説明する概念図である。以下に、送信側の情報通信端末100の情報の流れと、受信側の情報通信端末100の情報の流れに分けて説明する。

【0114】

(1) 送信側の情報通信端末100

まず、前提として、設定モジュール102aにおいて、疎結合XMLの生成に用いる各種のルールを生成する。ここで、図10は、設定モジュール102aにおける疎結合XMLの生成に用いる各種ルールの生成の概要を示す概念図である。

【0115】

例えば、企業情報に関するXML文書进行处理する場合を一例に説明すると、ルール設定処理部は、DTDリポジトリから企業情報用のDTDを参照して、ルール設定画面等を作成し、データ所有者による各要素の機密結合度の指定を行わ

せる。ルールビルダは、データ所有者が行った指定内容に基づいて、結合ルールおよびネーミングルール（情報通信端末 1 0 0 1 および情報通信端末 1 0 0 2）を自動生成する。なお、作成した各種のルールは、受信側の情報通信端末 1 0 0 に対して送信される。

## 【 0 1 1 6 】

ついで、図 5 に示すように、ユーザアプリケーションで作成されたオリジナル XML データは、XML ミドルウェア 1 0 2 c を介して、実行モジュール 1 0 2 b の入出力コネクタに送信される（ステップ S 5 0 1）。

## 【 0 1 1 7 】

入出力コネクタは、オリジナル XML データを、パーサに送信する（ステップ S 5 0 2）。

## 【 0 1 1 8 】

ついで、パーサは、オリジナル XML データの構文解析を行い、トークンを生成して、デバイダに送信する（ステップ S 5 0 3）。

## 【 0 1 1 9 】

ついで、デバイダは、設定モジュール 1 0 2 a が生成したルールに従って、XML データの分割を行い、また上述したように要素名の別名化を行い、疎結合 XML データを作成する。

## 【 0 1 2 0 】

ここで、図 9 は、デバイダにより実行される要素名の別名化、および、疎結合 XML データの作成の一例を示す概念図である。本事例は、オリジナル XML 9 0 1 に対して疎結合化を行い、2 つの XML データ 9 0 2 および 9 0 3 を生成する。同時にネーミングルールに従って別の要素名を設定している。第三者が、このような疎結合 XML からオリジナル XML を作り出すことは極めて難しい。

## 【 0 1 2 1 】

再び図 5 に戻り、デバイダは、IP アロケータの制御に基づいて IP の割り当てを行い、また、IP / ポートマネジャーの制御により資源の割り当てを行う。そして、上述したマルチルーティングを実行するために、複数の IP アロケータに疎結合 XML データを送信する（ステップ S 5 0 4）。

【 0 1 2 2 】

ついで、各 I・P アロケータはサーバに対して別の通信路を用いて受信側の情報通信端末 1 0 0 に対して疎結合 XML データを送信するように依頼する（ステップ S 5 0 5）。

【 0 1 2 3 】

サーバは、各通信路を用いて、疎結合 XML データを受信側の情報通信端末 1 0 0 に対して送信する（ステップ S 5 0 6）。

【 0 1 2 4 】

（2）受信側の情報通信端末 1 0 0

サーバは、ネットワーク 3 0 0 を介して疎結合 XML を受信すると（ステップ S 5 0 7）、疎結合 XML をパーサに対して送信する（ステップ S 5 0 8）。

【 0 1 2 5 】

ついで、パーサは、送信側の情報通信端末 1 0 0 から受信した DTD ファイルや、各種のルールに基づいて、別名化された要素名の復元したのち、疎結合 XML の構文解析を行い、トークンを生成してコンストラクタに送信する（ステップ S 5 0 9）。

【 0 1 2 6 】

ついで、コンストラクタは、結合ルールに基づいて、疎結合 XML からオリジナル XML を再構成して、入出力コネクタに送信する（ステップ S 5 1 0）。

【 0 1 2 7 】

ついで、入出力コネクタは、再構成した XML データを、XML ミドルウェア 1 0 2 c に送信すると、XML ミドルウェア 1 0 2 c は、ユーザアプリケーションに XML データを送信する（ステップ S 5 1 1）。

【 0 1 2 8 】

（システム構成－ネットワーク 3 0 0）

次に、図 1 のネットワーク 3 0 0 の構成について説明する。ネットワーク 3 0 0 は、情報通信端末 1 0 0 を相互に接続する機能を有し、例えば、インターネット等である。

【 0 1 2 9 】

## (他の実施の形態)

さて、これまで本発明の実施の形態について説明したが、本発明は、上述した実施の形態以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施の形態にて実施されてよいものである。

## 【 0 1 3 0 】

また、実施形態において説明した各処理のうち、自動的に行なわれるものとして説明した処理の全部または一部を手動的に行うこともでき、あるいは、手動的に行なわれるものとして説明した処理の全部または一部を公知の方法で自動的に行うこともできる。

この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種の登録データや検索条件等のパラメータを含む情報、画面例、データベース構成については、特記する場合を除いて任意に変更することができる。

## 【 0 1 3 1 】

また、情報通信端末 1 0 0 に関して、図示の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。

例えば、情報通信端末 1 0 0 が備える処理機能、特に制御部にて行なわれる各処理機能については、その全部または任意の一部を、CPU (Central Processing Unit) および当該 CPU にて解釈実行されるプログラムにて実現することができ、あるいは、ワイヤードロジックによるハードウェアとして実現することも可能である。

## 【 0 1 3 2 】

また、情報通信端末 1 0 0 は、さらなる構成要素として、マウス等の各種ポインティングデバイスやキーボードやイメージスキャナやデジタイザ等から成る入力装置 (図示せず)、入力データのモニタに用いる表示装置 (図示せず)、システムクロックを発生させるクロック発生部 (図示せず)、および、各種処理結果その他のデータを出力するプリンタ等の出力装置 (図示せず) を備えてもよい。

## 【 0 1 3 3 】

記憶部に格納される各種のデータは、RAM、ROM等のメモリ装置、ハードディスク等の固定ディスク装置、フレキシブルディスク、光ディスク等のストレ

ージ手段であり、各種処理やウェブサイト提供に用いる各種のプログラムやテーブルやファイルやデータベースやウェブページ用ファイル等を格納する。

【0134】

さらに、情報通信端末100の分散・統合の具合的形態は図示のものに限られず、その全部または一部を、各種の負荷等に応じた任意の単位で、機能的または物理的に分散・統合して構成することができる。例えば、各データを独立したデータベース装置として独立に構成してもよく、また、処理の一部をCGI (Common Gateway Interface) を用いて実現してもよい。

【0135】

この情報通信端末100の制御部は、その全部または任意の一部を、CPUおよび当該CPUにて解釈実行されるプログラムにて実現することができる。すなわち、記憶部には、OS (Operating System) と協働してCPUに命令を与え、各種処理を行うためのコンピュータプログラムが記録されている。このコンピュータプログラムは、RAMにロードされることによって実行され、CPUと協働して制御部を構成する。

【0136】

しかしながら、このコンピュータプログラムは、情報通信端末100に対して任意のネットワークを介して接続されたアプリケーションプログラムサーバに記録されてもよく、必要に応じてその全部または一部をダウンロードすることも可能である。このあるいは、各制御部の全部または任意の一部を、ワイヤードロジック等によるハードウェアとして実現することも可能である。

【0137】

また、本発明にかかるプログラムを、コンピュータ読み取り可能な記録媒体に格納することもできる。ここで、この「記録媒体」とは、フロッピーディスク、光磁気ディスク、ROM、EPROM、EEPROM、CD-ROM、MO、DVD等の任意の「可搬用の物理媒体」や、各種コンピュータシステムに内蔵されるROM、RAM、HD等の任意の「固定用の物理媒体」、あるいは、LAN、WAN、インターネットに代表されるネットワークを介してプログラムを送信する場合の通信回線や搬送波のように、短期にプログラムを保持する「通信媒体」

を含むものとする。

【0138】

また、「プログラム」とは、任意の言語や記述方法にて記述されたデータ処理方法であり、ソースコードやバイナリコード等の形式を問わない。なお、「プログラム」は必ずしも単一的に構成されるものに限られず、複数のモジュールやライブラリとして分散構成されるものや、OS (Operating System) に代表される別個のプログラムと協働してその機能を達成するものをも含む。なお、実施の形態に示した各装置において記録媒体を読み取るための具体的な構成、読み取り手順、あるいは、読み取り後のインストール手順等については、周知の構成や手順を用いることができる。

【0139】

また、ネットワーク300は、情報通信端末100を相互に接続する機能を有し、例えば、インターネットや、イントラネットや、LAN（有線／無線の双方を含む）や、VANや、パソコン通信網や、公衆電話網（アナログ／デジタルの双方を含む）や、専用回線網（アナログ／デジタルの双方を含む）や、CATV網や、IMT2000方式、GSM方式またはPDC／PDC-P方式等の携帯回線交換網／携帯パケット交換網や、無線呼出網や、Bluetooth等の局所無線網や、PHS網や、CS、BSまたはISDB等の衛星通信網等のうちいずれかを含んでもよい。すなわち、本システムは、有線・無線を問わず任意のネットワークを介して、各種データを送受信することができる。

【0140】

【発明の効果】

以上詳細に説明したように、本発明によれば、複数の要素の機密結合度を設定し、設定された機密結合度に基づいて、情報を複数の疎結合情報に分割するための分割ルールを設定し、設定された分割ルールに基づいて、情報を複数の疎結合情報に分割し、分割された複数の疎結合情報、および、設定された分割ルールを送信するので、送受信される情報の秘匿性を高めることができる情報交換システム、情報通信端末、情報交換方法、および、プログラムを提供することができる。



【 0 1 4 1 】

また、本発明によれば、複数の疎結合情報、および、分割ルールを受信し、受信した分割ルールに基づいて、複数の疎結合情報から情報を再構成するので、送受信される情報の秘匿性を高めることができる。

【 0 1 4 2 】

また、本発明によれば、送信手段は、複数の疎結合情報を複数の伝送経路を用いて送信するので、機密結合度が下げられて生成された複数の疎結合情報をそれぞれ別の通信路を用いて情報交換することができる。また、疎結合情報の対応関係を隠蔽し、送受信される情報の秘匿性をさらに高めることができる。

【 0 1 4 3 】

また、本発明によれば、要素の名称を別の名称とするためのネーミングルールを設定し、設定されたネーミングルールに基づいて、情報の要素の名称を別の名称にし、設定されたネーミングルールを送信するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

【 0 1 4 4 】

また、本発明によれば、ネーミングルールを受信し、受信した上記ネーミングルールに基づいて、別名化された情報の要素の名称を元の名称に変換するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

【 0 1 4 5 】

また、本発明によれば、情報は、XMLにより記載されているので、XMLデータの分解・再構成の容易性を活かしてXMLデータの機密結合度を下げ、秘匿性を高めることができる。

【 0 1 4 6 】

さらに、本発明によれば、DTDに定義されている要素について、要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定するので、

D T D に定義された X M L 情報の要素の内容に基づいて、効率的に機密結合度を設定できる。

【図面の簡単な説明】

【図 1】

本システムの全体構成の一例を示すブロック図である。

【図 2】

本システムの概要を示す概念図である。

【図 3】

本発明が適用される情報通信端末 1 0 0 の構成の一例を示すブロック図である。

【図 4】

本発明が適用される情報通信端末 1 0 0 の制御部 1 0 2 において実行されるソフトウェア構成の一例を示すブロック図である。

【図 5】

情報通信端末 1 0 0 における情報の流れの概要を説明する概念図である。

【図 6】

本システムにおける機密結合度の定義の一例を示す概念図である。

【図 7】

本発明の疎結合 X M L データのマルチルーティングの概要を示す概念図である。

【図 8】

本発明の要素名の別名化の概要を示す概念図である。

【図 9】

デバイダにより実行される要素名の別名化、および、疎結合 X M L データの作成の一例を示す概念図である。

【図 1 0】

設定モジュール 1 0 2 a における疎結合 X M L の生成に用いる各種ルールの生成の概要を示す概念図である。

【符号の説明】

1 0 0 情報通信端末

1 0 2 制御部

1 0 2 a 設定モジュール

1 0 2 b 実行モジュール

1 0 2 c XMLミドルウェア

1 0 4 通信制御インタフェース部

1 0 6 記憶部

1 0 8 入出力制御インタフェース部

3 0 0 ネットワーク

6 0 1、9 0 1 オリジナルXML

6 0 2、6 0 3、8 0 1、8 0 2、9 0 2、9 0 3 疎結合XML

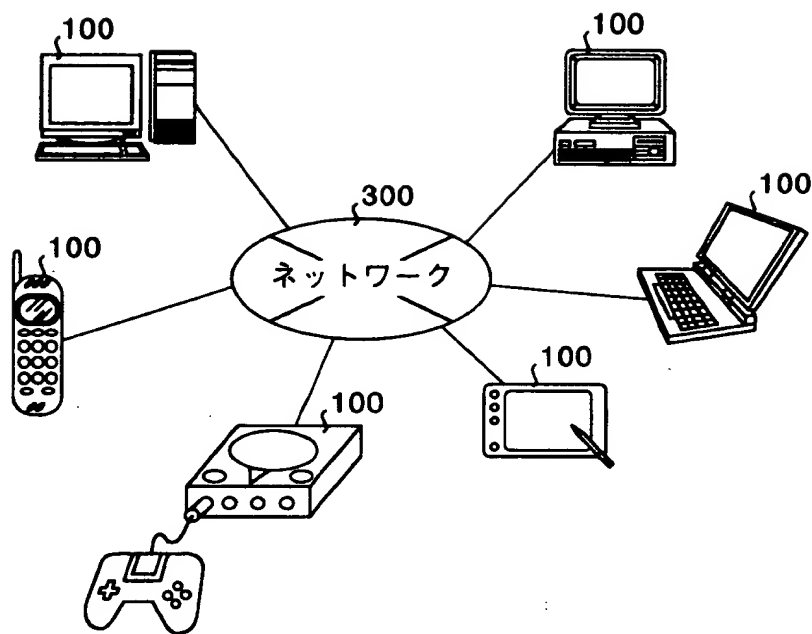
6 0 4、8 0 3、1 0 0 1、1 0 0 2 結合ルール

8 0 4、8 0 5 別名XML

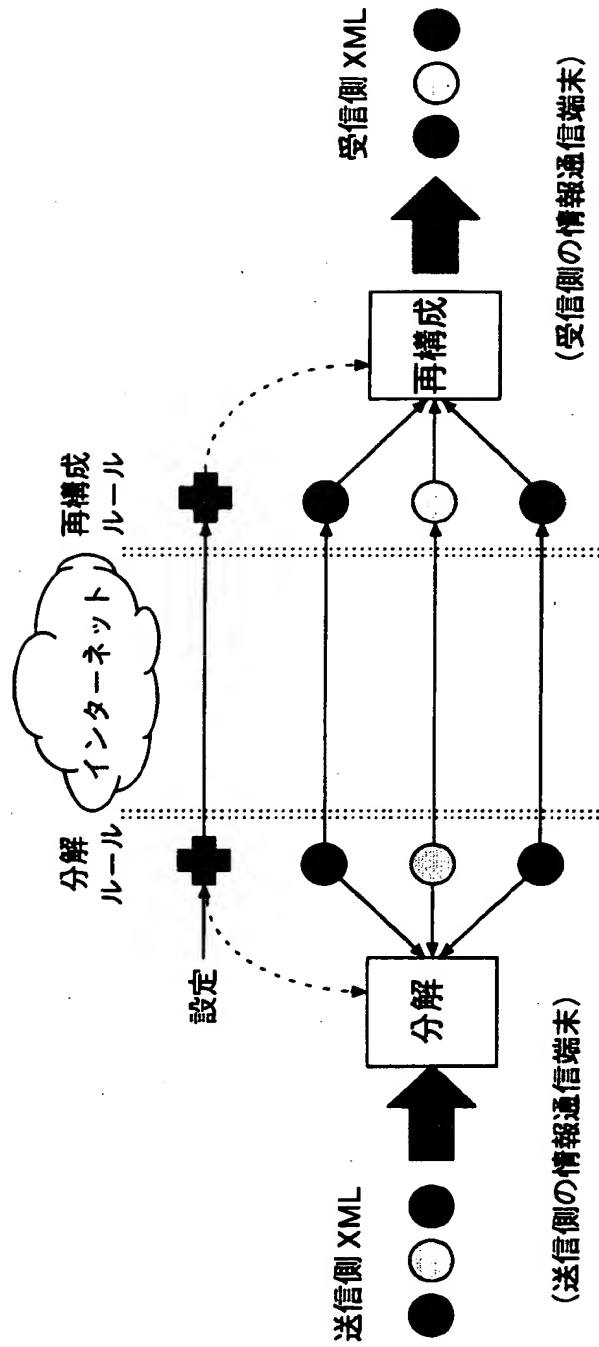
8 0 6 結合ルールおよびネーミングルール

【書類名】 図面

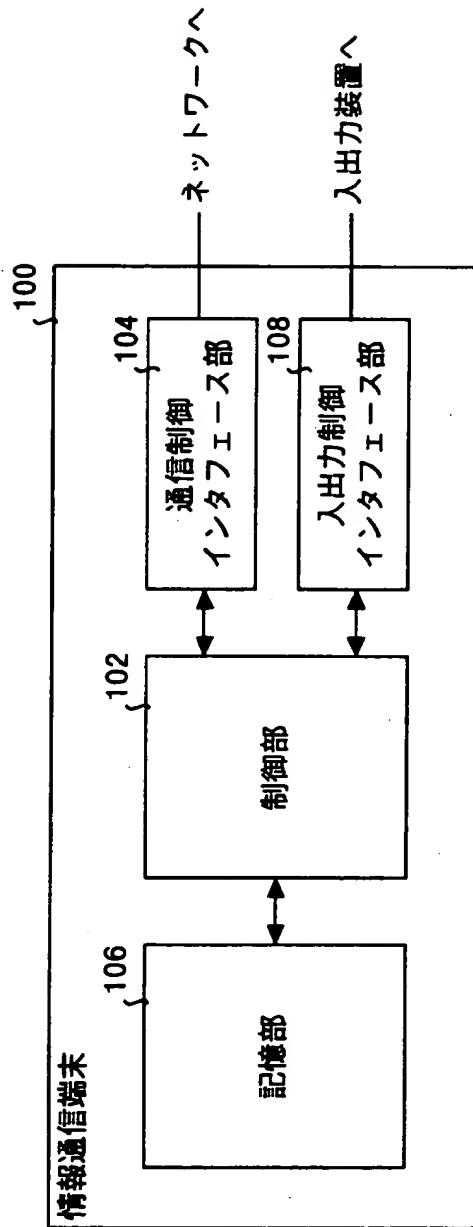
【図 1】



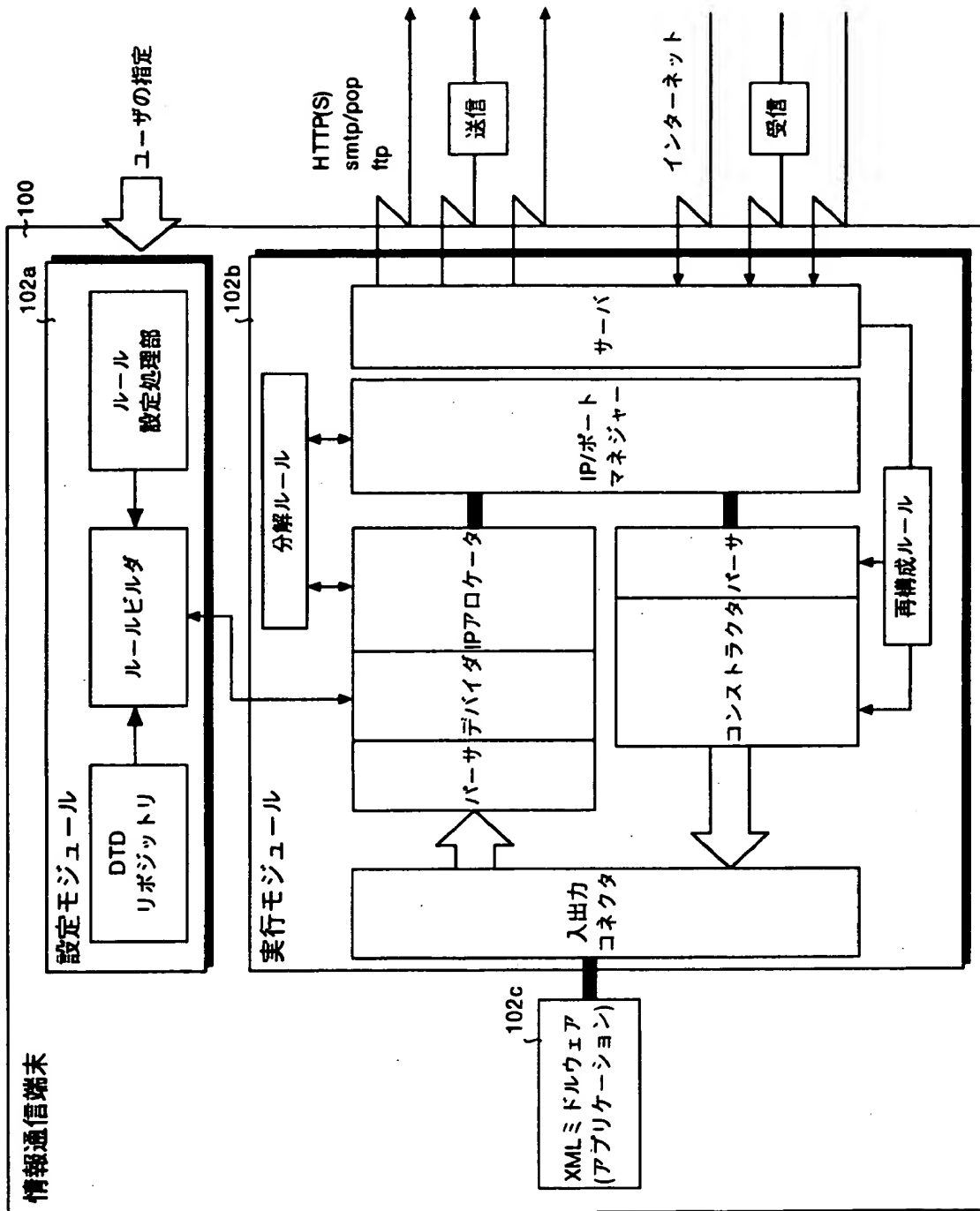
【図 2】



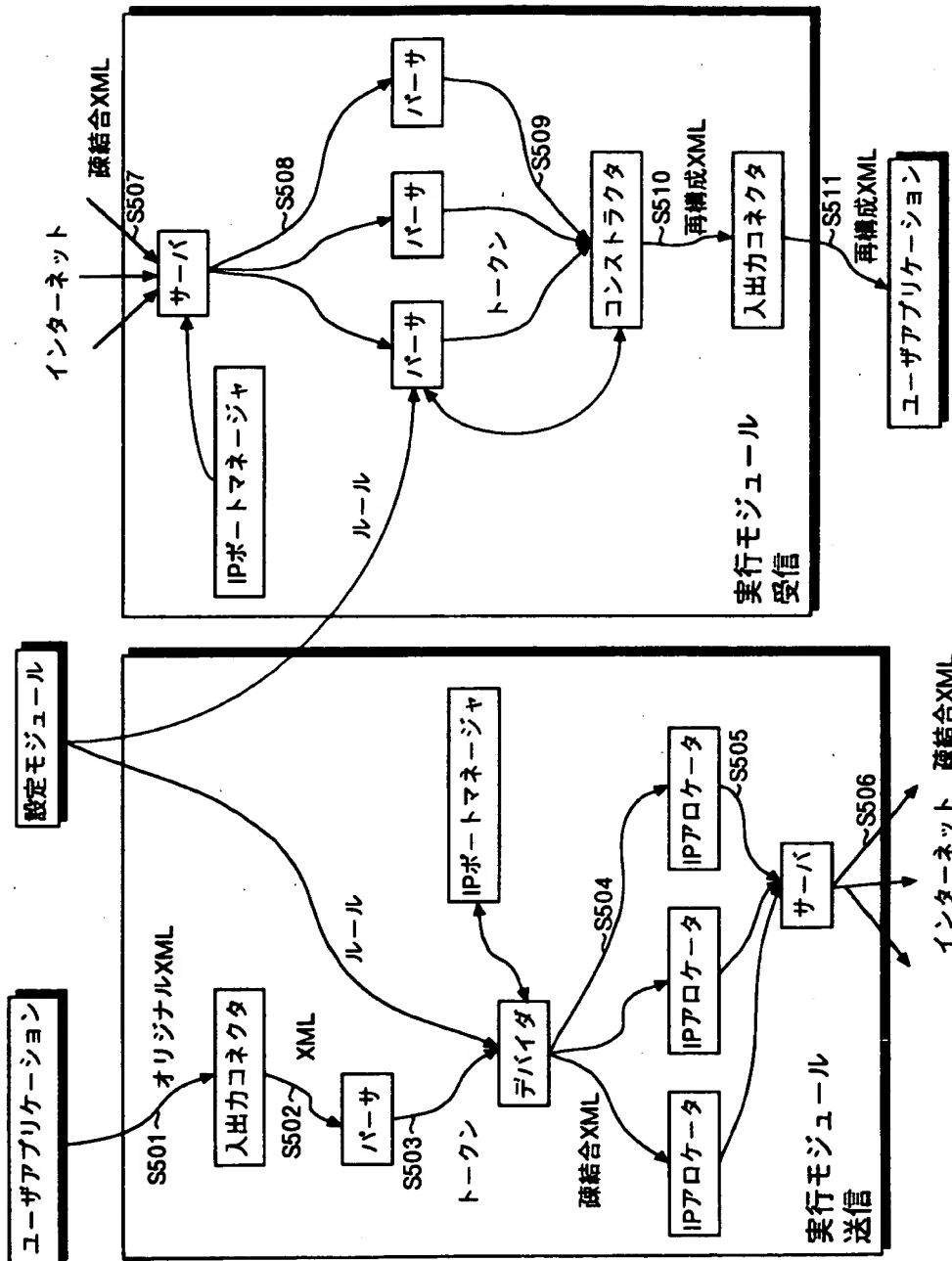
【図 3】



【図 4】

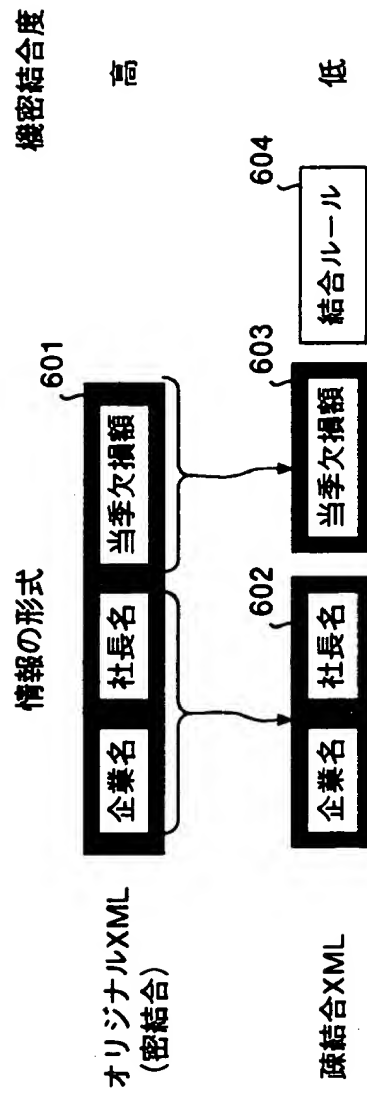


【図 5】

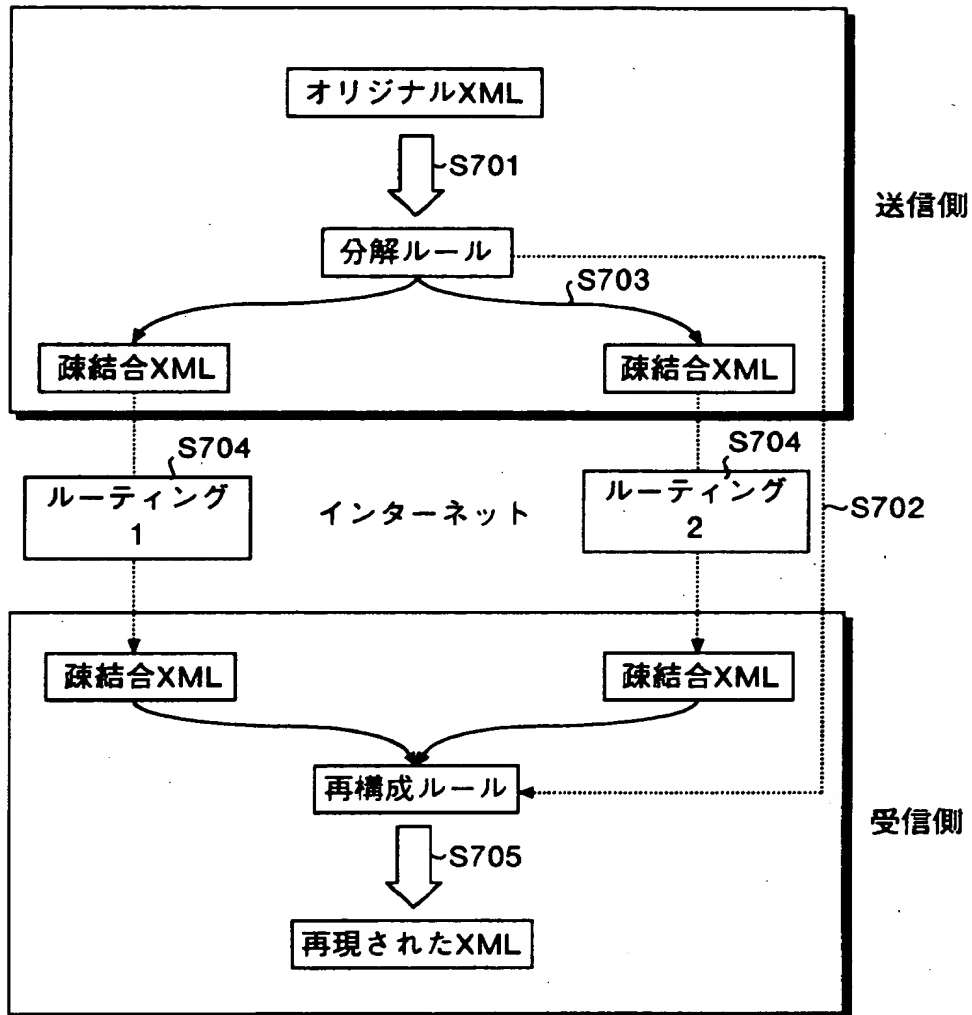




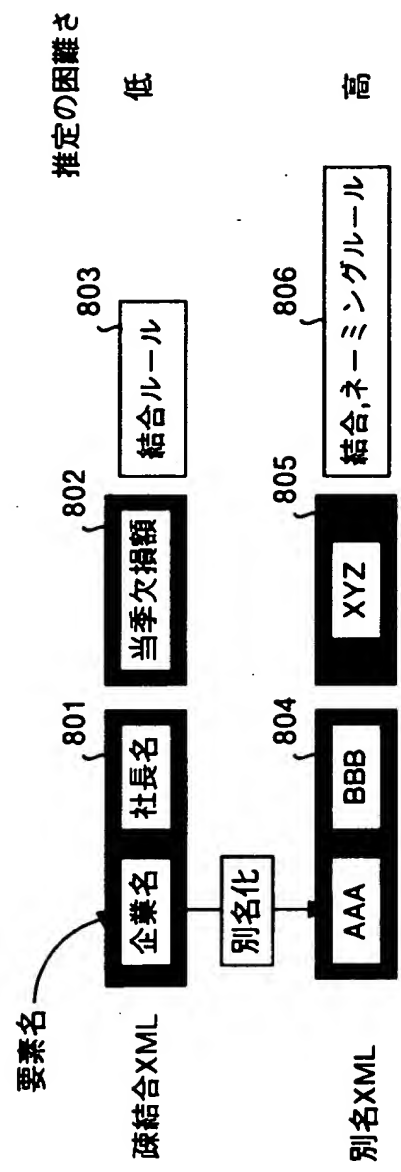
【図 6】



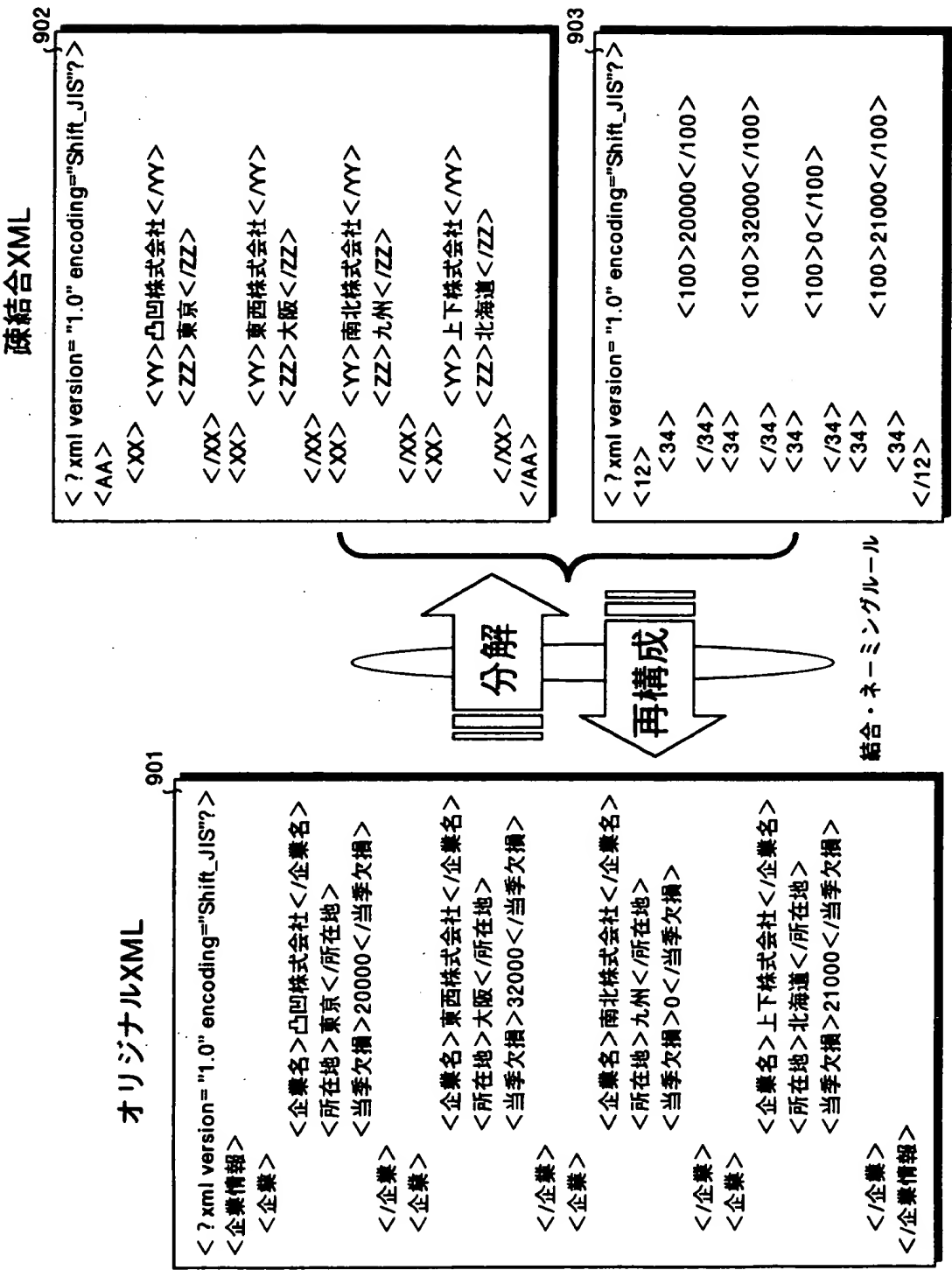
【図 7】



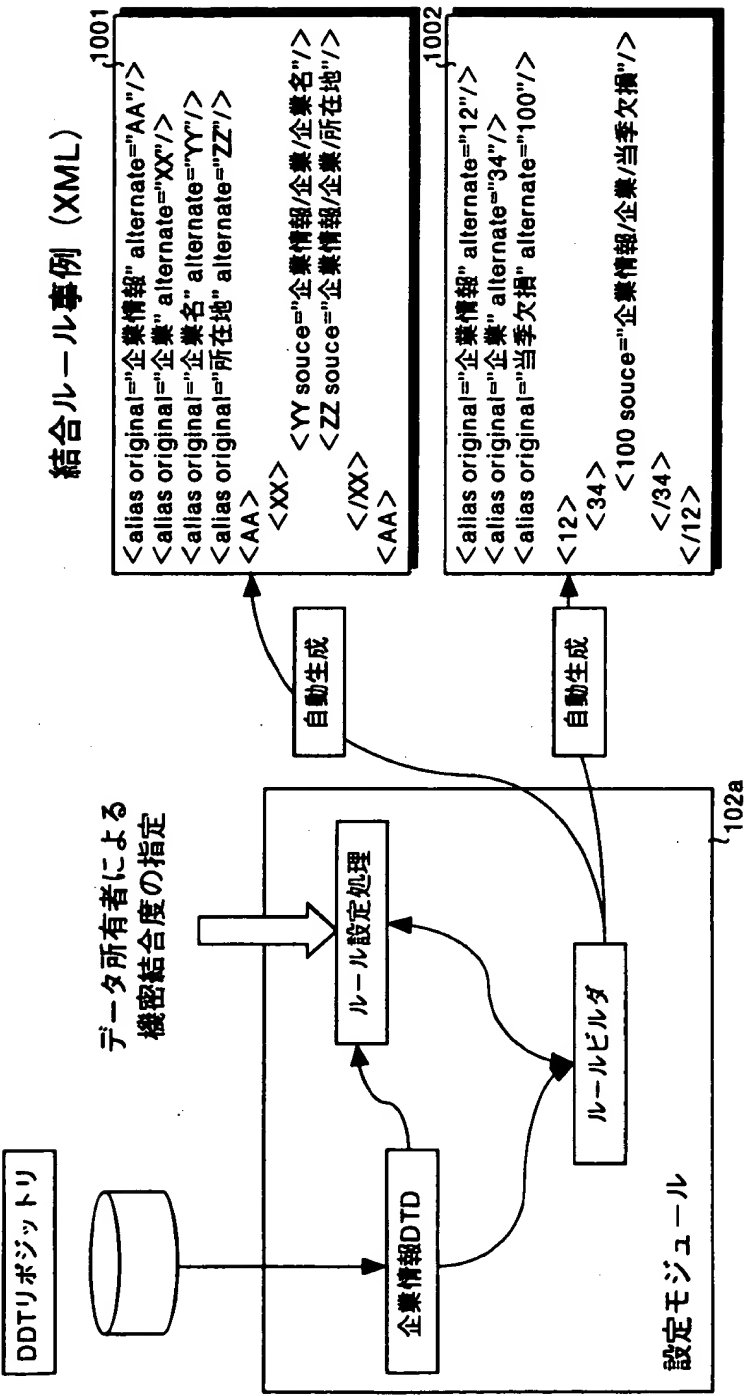
【図 8】



【図 9】



【図10】



【書類名】 要約書

【要約】

【課題】 比較的手軽な暗号化のような機密保護に加えて、万一それが破られても情報の秘匿性の保持を可能とするものであり、オープンなインターネットを利用しつつ秘匿性が高い情報の交換を安価に実現することのできるシステム等を提供することを課題とする。

【解決手段】 本発明にかかるシステムは、複数の要素を含む情報を送受信する情報通信端末 1 0 0 がネットワーク 3 0 0 を介して相互に接続される。送信側の情報通信端末は、複数の要素の機密結合度を設定し、設定された機密結合度に基づいて、情報を複数の疎結合情報に分割するための分割ルールを設定し、設定された分割ルールに基づいて、情報を複数の上記疎結合情報に分割し、分割された複数の疎結合情報および設定された分割ルールを送信する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [501125998]

1. 変更年月日 2001年 3月28日

[変更理由] 新規登録

住 所 千葉県船橋市習志野台2-21-4

氏 名 池田 実